In the Claims

This listing of claims replaces all prior versions and listings of the claims in the application.

Please amend the claims as follows:

1. (Currently Amended) A smartcard transaction system configured with a biometric security device, said system comprising:

a smartcard configured to communicate with a reader, wherein said reader and said biometric security device are configured to communicate with a host;

~~an integrated circuit device disposed within said smartcard and configured to communicate with said reader, said integrated circuit device comprising a common application and a second application, said second application being configured to store travel related information associated with a cardholder;~~

~~said second application comprising a common file structure and a partner file structure, wherein said partner file structure provides write access to a field within said partner file structure for a first partnering organization and denies write access to said field for a second partnering organization, and said common file structure provides write access for said first partnering organization and said second partnering organization to file in said common file structure;~~

said biometric security device comprising a biometric sensor configured to detect a proffered biometric sample to generate data representing said proffered biometric sample, said biometric sensor is configured to communicate with said system;

said system configured to use said data representing said proffered biometric sample as a variable in an encryption calculation to secure at least one of user data and transaction data; and,

a verification device configured to verify said proffered biometric sample to facilitate a transaction ~~using at least one of said partner file structure and said common file structure~~.

2. (Previously Presented) The smartcard transaction system of claim 1, wherein said biometric sensor is configured to communicate with said smartcard transaction system via at least one of said smartcard, said reader, and a network.

3. (Currently Amended) The smartcard transaction system of claim 1, wherein said system is configured to use said data representing said proffered biometric sample as at least one of a

private key and a public key to facilitate encryption security associated with said transaction. ~~partner file structure enables said first partnering organization to program said smartcard as a room key.~~

4. (Previously Presented) The smartcard transaction system of claim 1, wherein said biometric sensor is configured to store log data comprising at least one of a detected biometric sample, a processed biometric sample and a stored biometric sample, and wherein said biometric sensor is further configured to employ a security procedure when said proffered biometric sample differs from said log data.

5. (Original) The smartcard transaction system of claim 1, further including a database configured to store a data packet, wherein said data packet includes at least one of proffered and registered biometric samples, proffered and registered user information, terrorist information, and criminal information.

6. (Cancelled)

7. (Currently Amended) The smartcard transaction system of claim 1 ~~6~~, wherein said system is configured to use said data representing said proffered biometric sample in generating a message authentication code. ~~remote database is configured to be operated by an authorized sample receiver.~~

8. (Previously Presented) The smartcard transaction system of claim 1, further including a comparison device configured to compare said proffered biometric sample with a stored biometric sample.

9. (Previously Presented) The smartcard transaction system of claim 8, wherein said comparison device is configured to compare a biometric sample characteristic, said biometric sample characteristic including minutia, vascular patterns, prints, waveforms, odorants, nodal points, reference points, size, shape, thermal patterns, blood flow, and body heat.

10. (Cancelled)

11. (Cancelled)

12. (Currently Amended) The smartcard transaction system of claim 8 ~~11~~, wherein said stored biometric sample comprises a registered biometric sample and wherein said registered

biometric sample is associated with at least one of: personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information.

13. (Previously Presented) The smartcard transaction system of claim 12, wherein different registered biometric samples are associated with a different one of: personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information.

14. (Previously Presented) The smartcard transaction system of claim 12, wherein said biometric sample is primarily associated with a first user account, wherein said first account comprises personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information, and wherein a biometric sample is secondarily associated with a second user account, wherein said second account comprises personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information, where said second user account is different than said first user account.

15. (Original) The smartcard transaction system of claim 1, wherein said smartcard transaction system is configured to begin authentication upon verification of said proffered biometric sample.

16. (Currently Amended) The smartcard transaction system of claim 1, wherein said system is configured to use said data representing said proffered biometric sample in at least one of an asymmetric encryption algorithm and a symmetric encryption algorithm. ~~said first partner file structure includes card-holder preferences relating to at least one of rental cars, hotel reservations, and air travel~~.

17. (Previously Presented) The smartcard transaction system of claim 1, wherein said biometric sensor is configured to provide a notification upon detection of said proffered

biometric sample, and wherein said notification is at least one of a notification to a security vendor, a notification to a store employee, and a notification to a primary account holder that said primary account is being accessed.

18. (Currently Amended) The smartcard transaction system of claim 1, wherein said verification device is further configured to facilitate substantially simultaneous access to goods and initiation of authentication for a subsequent purchase of said goods ~~at least one of access, activation of a device, a financial transaction, and a non-financial transaction~~.

19. (Previously Presented) The smartcard transaction system of claim 1, wherein said verification device is configured to facilitate the use of a secondary security procedure, which includes sending a signal to said host to notify that a requested transaction would violate an established rule for said transponder.

20. (Currently Amended) The ~~transponder-reader~~ smartcard transaction system of claim 1, wherein said biometric sample is associated with a preset transaction limitation comprising at least one of a maximum transaction amount, minimum transaction amount, maximum number of transactions within a time period, maximum number of transactions, use by certain merchants, temporal limitation, geographic limitation, and use of non-monetary funds.

21. (Cancelled)

22. (New) The smartcard transaction system of claim 1, further comprising an integrated circuit device disposed within said smartcard and configured to communicate with said reader, said integrated circuit device comprising a common application and a second application, said second application being configured to store travel-related information associated with a cardholder; and

said second application comprising a common file structure and a partner file structure, wherein said partner file structure provides write access to a field within said partner file structure for a first partnering organization and denies write access to said field for a second partnering organization, and said common file structure provides write access for said first partnering organization and said second partnering organization to file in said common file structure.

23. (New) The smartcard transaction system of claim 1, wherein said system is further configured to use said data representing said proffered biometric sample as a message authentication code and as at least one of a private key and a public key to secure at least one of user data and transaction data.

24. (New) A smartcard transaction system configured with a biometric security device, said system comprising:

a smartcard configured to communicate with a reader, wherein said reader and said biometric security device are configured to communicate with a host;

said biometric security device comprising a biometric sensor configured to detect a proffered biometric sample to generate data representing said proffered biometric sample, said biometric sensor is configured to communicate with said system;

said system configured to use said data representing said proffered biometric sample as at least one of a variable in an encryption calculation, a private key, a public key, and a message authentication code to secure at least one of user data and transaction data; and,

a verification device configured to verify said proffered biometric sample to facilitate a transaction.